1. A data storage system for allowing an authorized user to process data stored therein and for preventing an unauthorized user from accessing said data, said system comprising:

at least one storage member configured to store said data therein;

at least one process member operationally coupled to said storage member and configured to process said data stored in said storage member; and

at least one guard member operationally coupled to said storage member and configured to effect at least one of degradation of at least a portion of said storage member and degradation of at least a portion of said data stored in said storage member.

2. The system of claim 1, wherein said storage member includes at least one of a magnetic unit configured to use magnetic characteristics to store said data therein and an optical unit configured to use optical characteristics to store said data therein.

3. The system of claim 1, wherein said process member includes at least one of a magnetic head and an optical head, each of said heads configured to perform processing of at least a portion of said data.

4. The system of claim 1 further comprising at least one access member configured to perform detection of at least one unauthorized attempt to access said data by said unauthorized user.

5. The system of claim 4, wherein said unauthorized attempt includes at least one of receiving an invalid login signal by said unauthorized user, movement of said storage member, uncoupling of said storage member from an article coupled thereto, and disassembly of said storage member.

6. The system of claim 5, wherein said receiving said invalid login signal includes at least one of receiving said invalid login signal for a pre-determined number of times and receiving said invalid login signal for a pre-determined period.

7. The system of claim 5, wherein said movement of said storage member is with respect to at least one of ground, said process member, said guard member, and said system.

8. The system of claim 5, wherein said uncoupling of said storage member from said article is at least one of electrical, optical, and mechanical.
said uncoupling of said storage member from said article.

9. The system of claim 5, wherein said storage member includes at least one memory unit and a housing, wherein said memory unit is configured to store said data at least one of magnetically and optically, wherein said housing is configured to retain at least a substantial portion of said memory unit therein, and wherein said disassembly of said storage member is to expose at least a portion of said memory unit out of said housing.

10. The system of claim 5, wherein said guard member is operationally coupled with said access member and configured to effect said degradation at least one of upon and after said detection of said unauthorized attempt.

11. The system of claim 10, wherein said guard number is configured to generate magnetic field around at least a portion of said storage member to effect said degradation.

12. The system of claim 10, wherein said guard number is configured to irradiate amplified light rays to effect said degradation.

13. The system of claim 10, wherein said guard number is configured to contact at least a portion of said storage member with at least one chemical agent to effect said degradation.

14. The system of claim 10, wherein said guard number is configured to mechanically damage at least a portion of said storage member to effect said degradation.

15. The system of claim 1, wherein said guard member includes at least one power supply unit configured to supply said guard member with at least one of electric power and mechanical power to effect said degradation.

16. A data process system for receiving a data storage device, for allowing an authorized user to store to said data storage device and to access data stored therein, and for preventing an unauthorized user from accessing said data, said system comprising:

at least one receiver member configured to receive said data storage device;

at least one process member operationally coupled to said receiver member and configured to process said data stored in said storage device received by said receiver member; and

at least one guard member operationally coupled to said receiver member and configured to effect at least one of degradation of at least a portion of said data storage device and degradation of at least a portion of said data stored in said data storage device.

17. A method for allowing an authorized access by an authorized user to data stored in a storage member and for preventing an unauthorized access by an unauthorized user to said data, said method comprising the steps of:

detecting an unauthorized attempt to access said data by said unauthorized user; and

degrading at least a portion of said data before said unauthorized user accesses said data.

18. The method of claim 17, said detecting step including at least one of the steps of:

receiving an invalid login signal by said unauthorized user;

sensing unauthorized movement of said storage member;

sensing uncoupling of said storage member from an article coupled thereto; and

sensing disassembly of said storage member.

19. The method of claim 17, said degrading step including none of the steps of:

encrypting at least a portion of said data; and

decrypting at least a portion of said data.

20. The method of claim 17, said degrading step including at least one of the steps of:

magnetically degrading said portion of said data;

optically degrading said portion of said data;

chemically degrading said portion of said data; and

mechanically degrading said portion of said data.